



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,696	01/24/2000	Shigeo Tsujii	FORM PTO-1082	6150

26021 7590 06/09/2005

HOGAN & HARTSON L.L.P.  
500 S. GRAND AVENUE  
SUITE 1900  
LOS ANGELES, CA 90071-2611

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/489,696

Applicant(s)

TSUJII ET AL.

Examiner

Thanhnga B. Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 04/04/2005 (RCE).
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 3-9 and 13-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 3-9 and 13-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 January 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
  - 2) ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Applicant's submission filed on April 04, 2005 has been entered. Claims 3-9 and 13-23 are pending. Claims 1-2 and 10-12 are canceled by applicant. Claims 3-4, 7-9, 13-15, 17, and 19-23 are amended. However, when reconsidering claims 9 and 21-23, examiner has found the non-statutory subject matter in claims 9 and 21-23. Therefore, upon further consideration, a new ground(s) of rejection is made herein.

#### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 9 and 21-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 recites "a computer readable recording medium that stores a program that generates at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext to said plaintext in a cryptographic communications system, comprising: first program code means for causing said computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity. the dividqd information allowine a diminished size of the secret key; and second program code means for causing said common keys using said components selected." Even through the preamble may sound like it has structural elements, the body of the claim recites a type of software programs and/or technology that allows easy upgrade to new modes and improve performance without the need to replace hardware. In addition, application's specification defines "a data signal embodied in a carrier wave may be the computer readable medium" (see page 11, lines 7-9 of Specification). This computer readable medium includes intangible media such as signals, carrier waves, transmissions optical waves, transmission media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claim 9 recites a non-statutory subject matter.

Claims 21-23 have limitations that are similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 3-9 and 13-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baba (US 5,987, 129), further in view of Matyas (US 4,736,423).

a. Referring to claim 3:

i. Baba teaches:

(1) a cryptographic, communications method for communications of information between entities wherein a plurality of centers are provided (as depicted in Figure 1 of Baba), each of which generates secret keys (or secret private keys) peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities, the divided information used to generate the secret keys allowing diminished sizes of the secret keys; one entity generates a first common key using a first component contained in at least one secret key generated by at least one of the plurality of centers, the secret key being peculiar to the one entity, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts said ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity [**i.e., as shown in Figure 1, a the cryptosystem includes a center or central facility 1, which is a basic main constituent of the**

system, a plurality of entities 2 which are subscribed to the cryptosystem for communication with each other, and a network 3 such as the Internet, a personal computer communication network, or the like through which the center 1 and the entities 2 are connected to communicate with each other. The center 1 and the entities 2 include computers such as personal computers for effecting actual communications and data processing and users of those computers. In the cryptosystem on the network 3, as shown in Figure 2, the entities 2 (represented by  $i, j, \dots$  in Figure 2) have respective peculiar identifiers  $y_i, y_j, \dots$  (described in detail later on). If  $i \neq j$ , then  $y_i \neq y_j$ . The entities 2 ( $i, j, \dots$ ) have been given, by the center 1, respective secret private keys  $X_i, X_j, \dots$  (described in detail later on and hereinafter referred to as a "secret private key  $X_n$ " if necessary) which are peculiar to the respective entities 2 and generated by the center 1 based on the respective identifiers  $y_i, y_j, \dots$  (hereinafter referred to as an "identifier  $y_n$ " if necessary). For cryptographic communications between any arbitrary entities  $i, j$ , a common cryptokey  $K_{ij}$  for encrypting communication data (on the transmitting side) and decrypting communication data (on the receiving side) is generated for the entities  $i, j$  using the secret private keys  $X_i, X_j$  of the entities  $i, j$ . Using the generated common cryptokey  $K_{ij}$ , the encrypted communications are carried out between the entities  $i, j$ . The cryptosystem for carrying out the above cryptographic communications described in detail with reference to Figures 3 through 8 (column 8, lines 66-67 through column 12, lines 34)]. In addition, if there are a plurality of centers, then " $x_i$ " in the equation  $V_i(\eta) = x_i \cdot f(\eta)$  is replaced with the summation of the matrix  $x_i$  determined as described above for each of the centers (column 16, lines 8-10)].

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provided in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret

Art Unit: 2135

key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES **(column 3, lines 65-68 through column 4, lines 1-3 of Matyas)**. Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made **(column 6, lines 53-68 through column 7, lines 1-6 of Matyas)**.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards **(column 1, lines 9-14 of Matyas)**.

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card

Art Unit: 2135

must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. **(column 3, lines 40-52 of Matyas).**

b. Referring to claim 4:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

c. Referring to claim 7:

i. Baba teaches:

(1) storage means at each entity for storing secret keys peculiar to each respective entity produced for respective pieces of information resulting from division of information specifying each of said respective entities, the divided information used to generate the secret keys allowing diminished sizes of the secret keys; **[i.e., referring to Figure 1, When each entity 2 receives the secret private key  $X_n$  and the identifier transformation algorithm, it stores them secretly in a suitable storage device of its own computer (column 10, lines 14-16)];**

(2) selection means for selecting components corresponding to pieces of information specifying opposite entities to be communicated with, from among the secret keys stored; and means for generating said common keys using said components so selected **[i.e., in the cryptosystem, the secret private key of each entity 2 is generated and a common cryptokey is generated according to a linear transformation or scheme. It is assumed that  $X_{if}$  represents the secret private key of an entity  $i$  for the generation of a common cryptokey shared by  $f$  entities 2. According to a general concept for constructing the above linear scheme, that is "selection", an  $f$ -input symmetric transformation  $g$  (which is a symmetric function having  $f$  variables) is arbitrarily selected (column 15, lines 12-20)].**

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES **(column 3, lines 65-68 through column 4, lines 1-3 of Matyas)**. Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made **(column 6, lines 53-68 through column 7, lines 1-6 of Matyas)**.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm)



crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards (**column 1, lines 9-14 of Matyas**).

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. (**column 3, lines 40-52 of Matyas**).

d. Referring to claim 8:

i. Baba teaches:

(1) a plurality of centers that generate secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities and that sends said secret keys to said entities, the divided information used to generate the secret keys allowing diminished sizes of the secret keys [**i.e., referring to Figure 3, generating, in the center, that could be a plurality of centers (see column 16, line 8), a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities (column 2, lines 50-57)]**]; and

(2) a plurality of entities each of which generates a common key employed mutually in said encryption and decryption processing when communicating with another entity, using a component corresponding to a divided

specified information to each entity, contained in own secret key sent from the centers, the component corresponding to one or more pieces of information specifying said another entity [i.e., **a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities (column 2, lines 46-63)]].**

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES (column 3, lines 65-68 through column 4, lines 1-3 of Matyas). Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public

Art Unit: 2135

modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made (**column 6, lines 53-68 through column 7, lines 1-6 of Matyas**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards (**column 1, lines 9-14 of Matyas**).

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. (**column 3, lines 40-52 of Matyas**).

e. Referring to claim 9:

i. Baba teaches:

(1) a computer readable recording medium that stores a program that generates at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext to said plaintext in a cryptographic communications system, comprising: first program code means for causing said computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity, the divided information allowing diminished sizes of the secret keys; and second program code means for causing said computer to generate said common keys using said components selected [i.e., as shown in **Figure 8, the computer of each of the entities 2 comprises a keyboard 4, a main unit 5 made up of a CPU, a RAM, a ROM, etc., and a data base 6 comprising a hard disk, that is “a computer readable recording medium”, or the like for storing the secret private key xn, the identifier transformation algorithm, plaintexts such as sentences, programs (which can include “first program code and second program code”), etc., and encrypted communication texts (column 12, lines 19-25)].**

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES (**column 3, lines 65-68 through column 4, lines 1-3 of Matyas**). Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public

Art Unit: 2135

modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made (**column 6, lines 53-68 through column 7, lines 1-6 of Matyas**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards (**column 1, lines 9-14 of Matyas**).

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications, either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. (**column 3, lines 40-52 of Matyas**).

f. Referring to claim 13:

i. This claim has limitations that is similar to those of claims 3, thus it is rejected with the same rationale applied against claims 3 above.

g. Referring to claim 22:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

h. Referring to claims 5 and 6:

i. Baba does not explicitly teaches:

(1) wherein computation formulas for generating secret keys at said centers.

(2) wherein computation formulas for generating common keys at said entities.

ii. However, Baba does imply or suggest:

(1) as shown in Figure 3, cryptographic communications are carried out between the entities i, j after the center 1 generates and distributes the secret private key  $X_n$  in a preparatory stage. In the preparatory stage, the center 1 generates a center algorithm, that is "computation formulas", which serves as a basis for generating the secret private key  $X_n$  of each entity when the center 1 is established or the cryptosystem is updated (step 1) (**column 7, lines 62-67 through column 8, lines 1-2**).

(2) referring back to Figure 3, when the entities 2 (i, j, . . . ) are subscribed to the cryptosystem, the center 1 generates a secret private key  $X_n$  peculiar to each of the entities 2 and an identifier transformation algorithm, that is "computation formulas" for generating a common cryptokey  $K_{ij}$  (**column 8, lines 66-67 through column 9, lines 1-3**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) fully define by an expression containing mathematical function/formulas as in the center algorithm and identifier transformation algorithm of Baba (**column 8, lines 58-65**).

iv. The ordinary skilled person would have been motivated to:

(1) fully reveal or express containing mathematical function/formulas about the generation of secret key and common key as shown in

Figure 3 of Baba, a flowchart of an operation sequence of the cryptosystem shown in Figure 1 of Baba.

i. Referring to claim 14:

i. This claim has limitations that is similar to those of claims 5, thus it is rejected with the same rationale applied against claims 5 above.

j. Referring to claim 15:

i. This claim has limitations that is similar to those of claims 5, thus it is rejected with the same rationale applied against claims 5 above.

k. Referring to claims 16 and 18:

i. These claims have limitations that is similar to those of claim 6, thus they are rejected with the same rationale applied against claim 6 above.

l. Referring to claim 17:

i. This claim has limitations that is similar to those of claims 3 and 5, thus it is rejected with the same rationale applied against claims 3 and 5 above.

m. Referring to claim 19:

i. Baba teaches:

(1) a common key generator provided at entities in a cryptographic communications system for generating a common key to be used in processing to encrypt plaintext to ciphertext and in processing to decrypt ciphertext back to plaintext [i.e., referring to Figure 8, the main unit 5 includes as its functions a common key generator 7 for generating a common key, an encrypting and decrypting processor 8 for encrypting and decrypting communication data (column 12, lines 25-28)], comprising:

(2) This claim also has limitations that is similar to those of claims 6 and 7, thus it is rejected with the same rationale applied against claims 6 and 7 above.

ii. Though Baba teaches the claimed subject matter, Baba does not explicitly mention the generator which generates the secret keys (column 9, lines 7-20 and column 10, lines 52-65) could reduce the sizes of the secret keys. On the other hand, Matyas teaches:

(1) A technique is provide in Matyas' invention for reducing RSA crypto variable storage from 1200 bits (400-bit public key, 400-bit secret key, and 400-bit modulus) to 10 bits. Of the 106 bits, only 56 bits (denoted X) must be kept secret. The size of X has thus been chosen to maintain equivalence with the DES **(column 3, lines 65-68 through column 4, lines 1-3 of Matyas)**. Furthermore, Matyas' invention shows a method that allows the public key and modulus (amounting to 800 bits) to be regenerated from only 260 bits of public information. Thus, by decrypting these 260 bits, no more than 400 bits of data will be produced that requires transmission. This is the minimum that must be transmitted and represents the best that could be done under any conditions. However, since 260 bits must be padded with roughly 140 bits to form a full block before decryption with the secret key and public modulus of the key distribution center can be performed, there are, in effect, 140 extra bits available that can be used very effectively to enhance the security of the distribution protocol at no extra penalty in terms of the number of transmitted bits. For example, these bits could include 56 redundant zero bits to allow the block of recovered data to be properly authenticated, a time-variant parameter or sequence number to allow the receiver to test that the crypto variable is not stale and is received in proper sequence, and an ID of the user to whom the public key and modulus belongs to insure that the crypto variables belong to the user for whom the request is being made **(column 6, lines 53-68 through column 7, lines 1-6 of Matyas)**.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matyas into Baba's invention to encryption techniques for code stored on magnetic stripe cards and, more particularly, to techniques for reducing RSA (Rivest, Shamir, and Adleman algorithm) crypto variable storage size so that the RSA algorithm is compatible with magnetic stripe cards **(column 1, lines 9-14 of Matyas)**.

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matyas into Baba's invention since in order for the RSA algorithm to be workable in banking applications,



either a new magnetic stripe card with more storage must be developed or a more efficient way to store the secret key and modulus on the present magnetic stripe card must be found. Being incompatible with present magnetic stripe cards is a major disadvantage that would most likely impede the acceptance of public key algorithms. Applications involving personal keys (an especially important feature of public key cryptography) will thus be negatively impacted unless efficient techniques for storing parameters on the magnetic stripe card can be found or present card storage capabilities are extended. **(column 3, lines 40-52 of Matyas).**

n. Referring to claim 20:

i. This claim has limitations that is similar to those of claims 6 and 8, thus it is rejected with the same rationale applied against claims 6 and 8 above.

o. Referring to claim 21:

i. This claim has limitations that is similar to those of claims 6 and 9, thus it is rejected with the same rationale applied against claims 6 and 9 above.

p. Referring to claim 23:

i. This claim has limitations that is similar to those of claims 6 and 9, thus it is rejected with the same rationale applied against claims 6 and 9 above.

**Conclusion**

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kaufman et al (US 5,764,772) discloses differential work factor cryptographic method, system, and data structure for reducing but not eliminating the work factor required by an authority to break an encrypted message encrypted with a secret encryption key (see abstract).

b. Ganesan et al (US 5,588,061) discloses a method for improving an RSA cryptosystem by generating a user private exponent key, having an associated modulus N, and a user public exponent key for each user of the system (see abstract).

c. Liu (US 5,539,827) discloses a cryptographic device and method provide a repertoire of mappings and associated inverse mappings between plaintext and ciphertext vectors (see abstract).

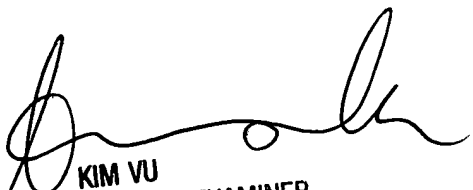
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

April 23, 2005



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100